Optimizing operations

Leading through a crisis

Webinar report

Business
Services

With one third of the entire planet on lockdown due to the recent pandemic, organizations have been racing to work out how they can maximize the performance of their networks, while providing users with remote access and ensuring security across the business.

In normal circumstances, around 63% of organizations have remote workers. Adequate bandwidth and licenses are there for users as part of a flexible working environment. But what happens in a crisis, when all employees suddenly have to work from home? Orange Business Services ran a **webinar** to look the options. Check out our nine tips on page 4.

Contingency plans and best practices need to be in place to optimize operations, ensure security and monitor performance for remote workers in a major disruption. Otherwise the outcome could be catastrophic for your organization. At best there will be a huge degradation in performance, at worst the network and business will grind to a halt.

Most organizations will have spent significant time formulating business continuity and disaster recovery plans. But many of these blueprints do not take into account the unique issues of having an entire organization working from home overnight.

Doing more with less

Any crisis forces an organization to do more with less and be prepared to move and adapt rapidly. Employees must learn how to collaborate remotely, even in roles where teleworking was not previously thought feasible. IT and security managers need to provide users with access to the performance and applications they are used to, while protecting them on their home networks far away from the security of their own organization's infrastructure.

Optimize your network for remote access at scale

When the bulk of employees are working remotely, it puts immense pressure on IT infrastructures. Most remote access and business continuity plans are not designed to handle a crisis involving all employees at the same time.

Don't let this disruption overwhelm your infrastructure. First, make the most of your remote access infrastructure by increasing your VPN licenses for a higher number of concurrent users. If you are still short on connections, you can leverage your existing firewall and appliances, for example, as they usually integrate a remote access function.

Second, optimize bandwidth by limiting bandwidth-hungry recreational traffic going through the corporate network, such as social networking.

Finally, consider using a mix of security, network, and cloud solutions to quickly scale your remote access, such as by using the Orange virtual remote access gateways. These gateways exploit the scalability and elasticity of the cloud and are available with minimal commitment.

You can only manage what you can see

Without proper monitoring and visibility on the remote workforce productivity, there is no insight into business continuity performance.

With employees working from home, and sometimes accessing applications without using the company's network, the only possible data capture point for meaningful data harvesting is the user end point.

End User Experience monitoring solutions allow for in-depth visibility into which applications users are using (to enforce security and compliance), and how their experience is while using them (what's the impact on productivity?). They also provide full visibility on the endpoint performance itself.

IT Support organisations are able to diagnose performance issues faster and better (distinguish between endpoint, home office connectivity, network/VPN, application issues) and prioritize incidents depending on the number of people impacted.

Consider deploying such a solution to monitor the "new normal", where more and more users will work remotely.

Nine tips to keep your business working remotely during a crisis

Is your business now prepared to work through any major global disruption? The COVID-19 pandemic has required that your employees work from home or off-site in a very short timeframe. In our webinar, we identified nine key considerations to make this enforced period of teleworking a success.

1 **Use secure connections:** expand your current remote access infrastructure to ensure that your employees have a secure VPN connection to the corporate network.

2 **Assess your organization's threat model and security policies:** in a period of disruption, the threat to your business is likely to look very different from yesterday.

3 **Establish security response procedures and systems:** breaches are more likely in a crisis and the response may be constrained. Also review your back up and discovery processes, as ransomware and extortion tactics are a bigger risk and procedures more challenging off-site.

4 **Re-establish visibility of your remote endpoints:** this needs to cover security, vulnerability monitoring, attack detection, performance, system health and application performance.

5 **On-boarding new users:** you will have profiles for new users that have never worked remotely before. Make sure you have the governance and policies in place to install the VPN client remotely and provide them with guidance on how to download and configure it.

6 **Talk with your users:** provide them with rational, balanced information they can use to assess risks themselves and make considered decisions. Communicate end-user training clearly, highlighting what is allowed and what is not in working remotely.

7 **Review the patching of remote endpoints and BYOD:** specific patches that make user endpoints exploitable are the key concern. Every device that is patched reduces the risk vector. In lieu of a viable central patching solution, advise users directly of essential patches and get them to apply them directly.

8 **Optimize use of existing bandwidth:** limit recreational traffic going through your corporate network. You can also offload this traffic completely to the internet using "split tunneling". Be warned that you will be bypassing the corporate secure internet gateway, potentially exposing the endpoints to additional threat if you do this. Ensure endpoints are hardened and consider endpoint detection and response solutions.

9 **Finally, stay in touch with your suppliers, contractors and even your competition:** reach out, maintain communications, and stay in touch. A crisis is a time for forming communities, working together and collaborating to understand risk.

Our remote working, performance monitoring and cyberdefense solutions can get your workforce up and running swiftly and limit the impact of a major disruption. To listen to a full recording of the webinar visit: https://www.brighttalk.com/webcast/15163/396910

orange™

Business
Services

Sources:

1. Statista – 2020 (provided by OBS)
2. Gartner Toolkit: remote working policies 2019public-private-partnerships-smart-cities-funding-finance.pdf